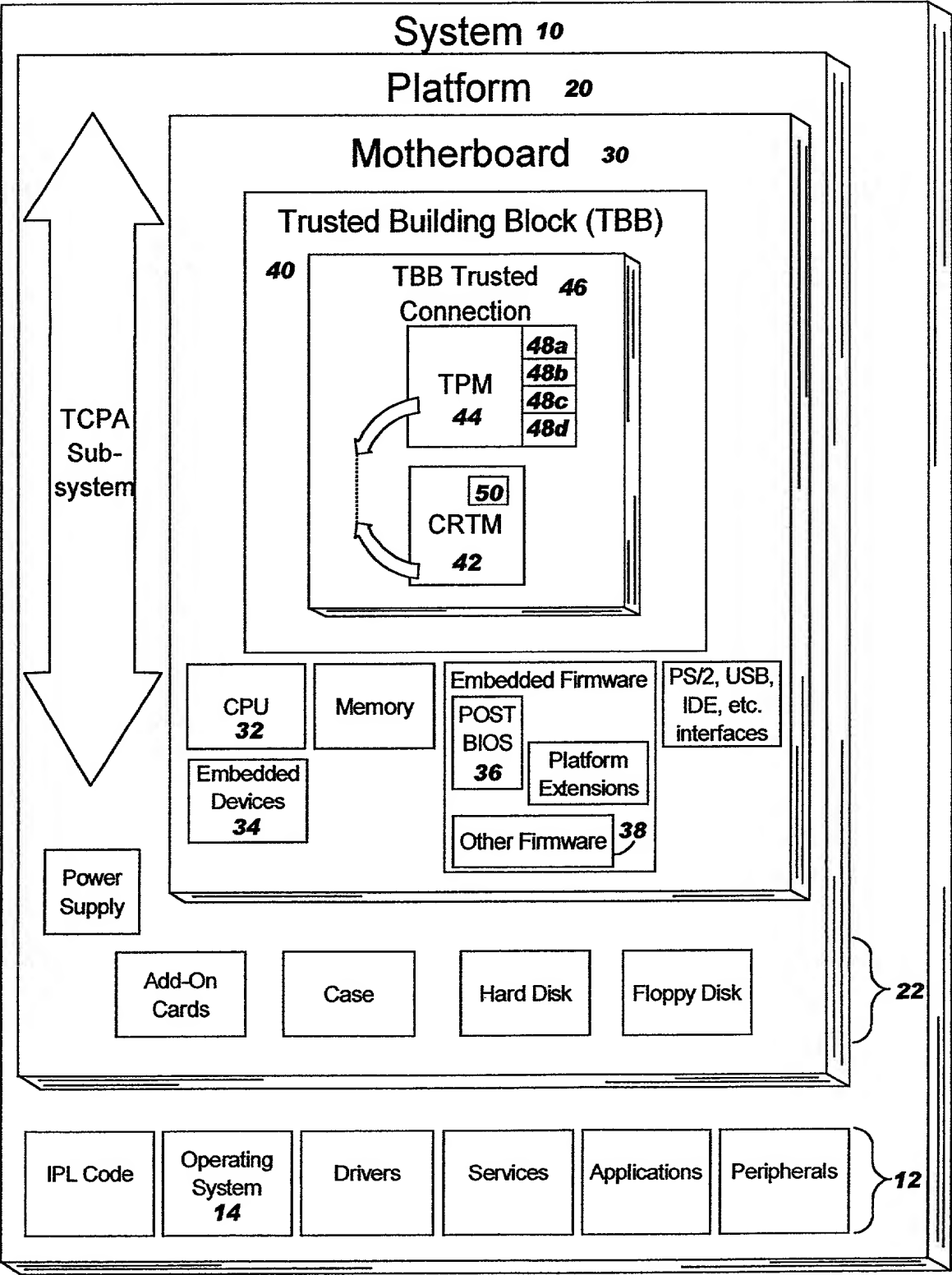


FIG. 1



09978331-101601

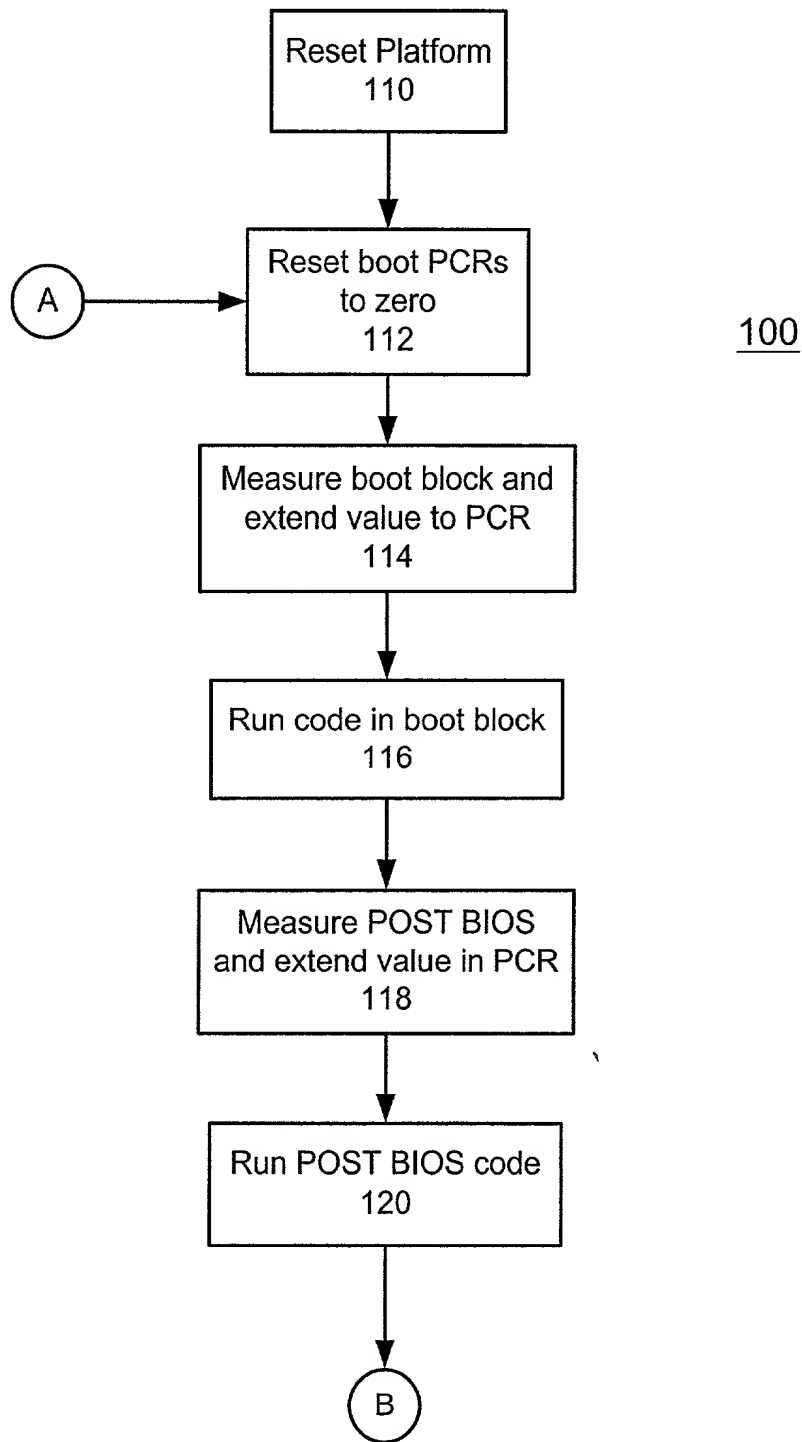


FIG. 2A

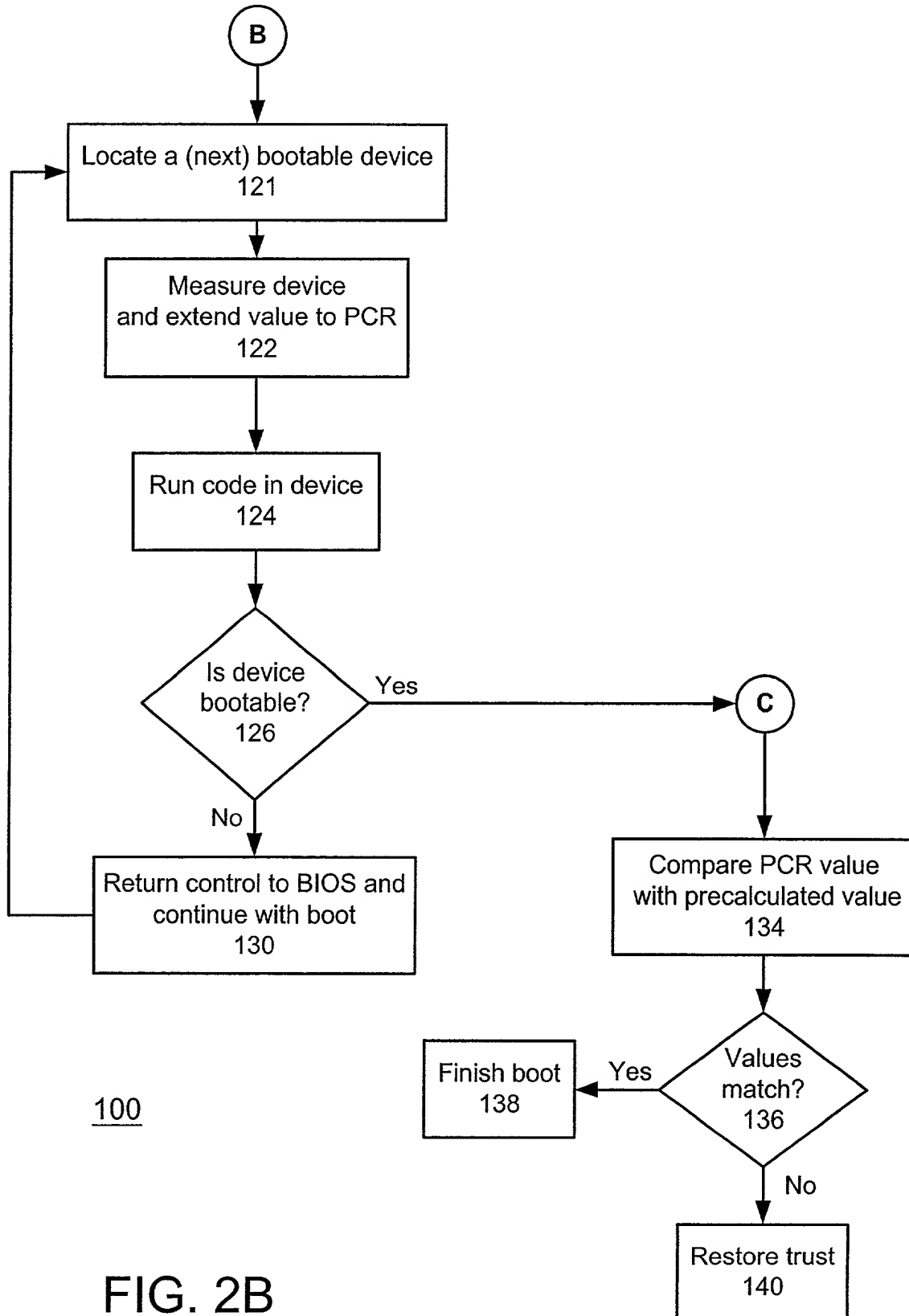


FIG. 2B

RPS920010054  
D. C. Cromer et al.  
Method and System for Tracking a Secure Boot  
in a Trusted Computing Environment

TPM 44'	Boot PCR 48a	Shadow PCR 48a'
	48b	
	48c	
	48d	

FIG. 3

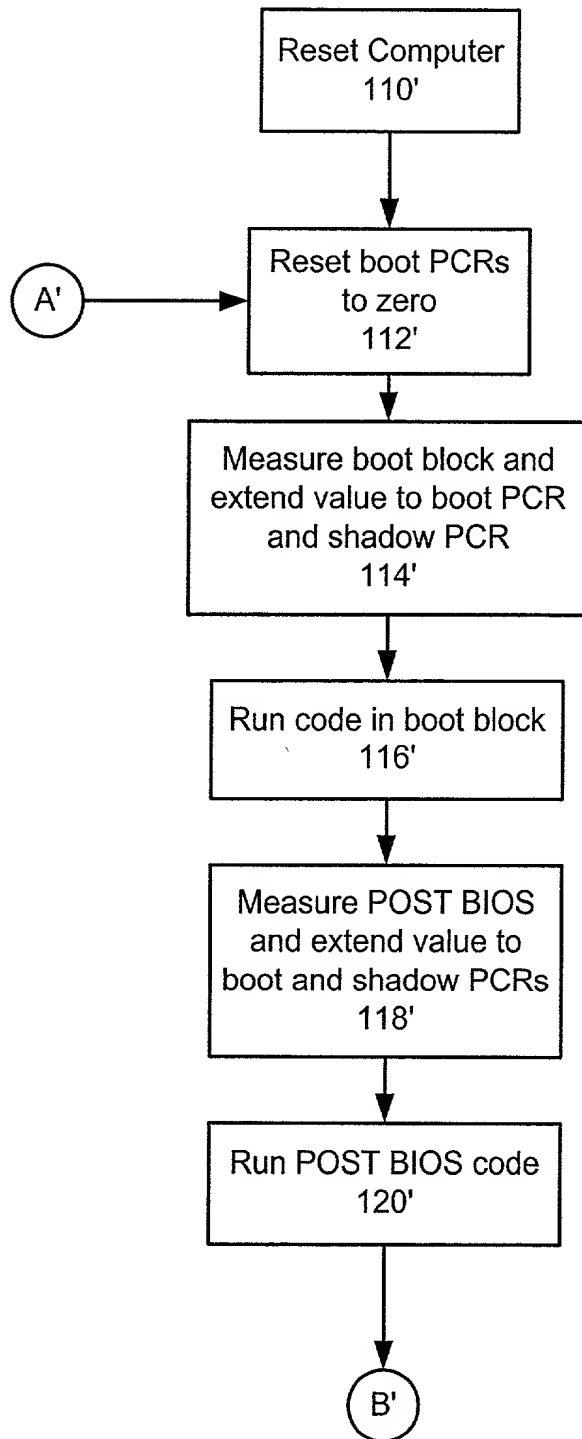


FIG. 3A

09978361-101601  
T09T T8E4660

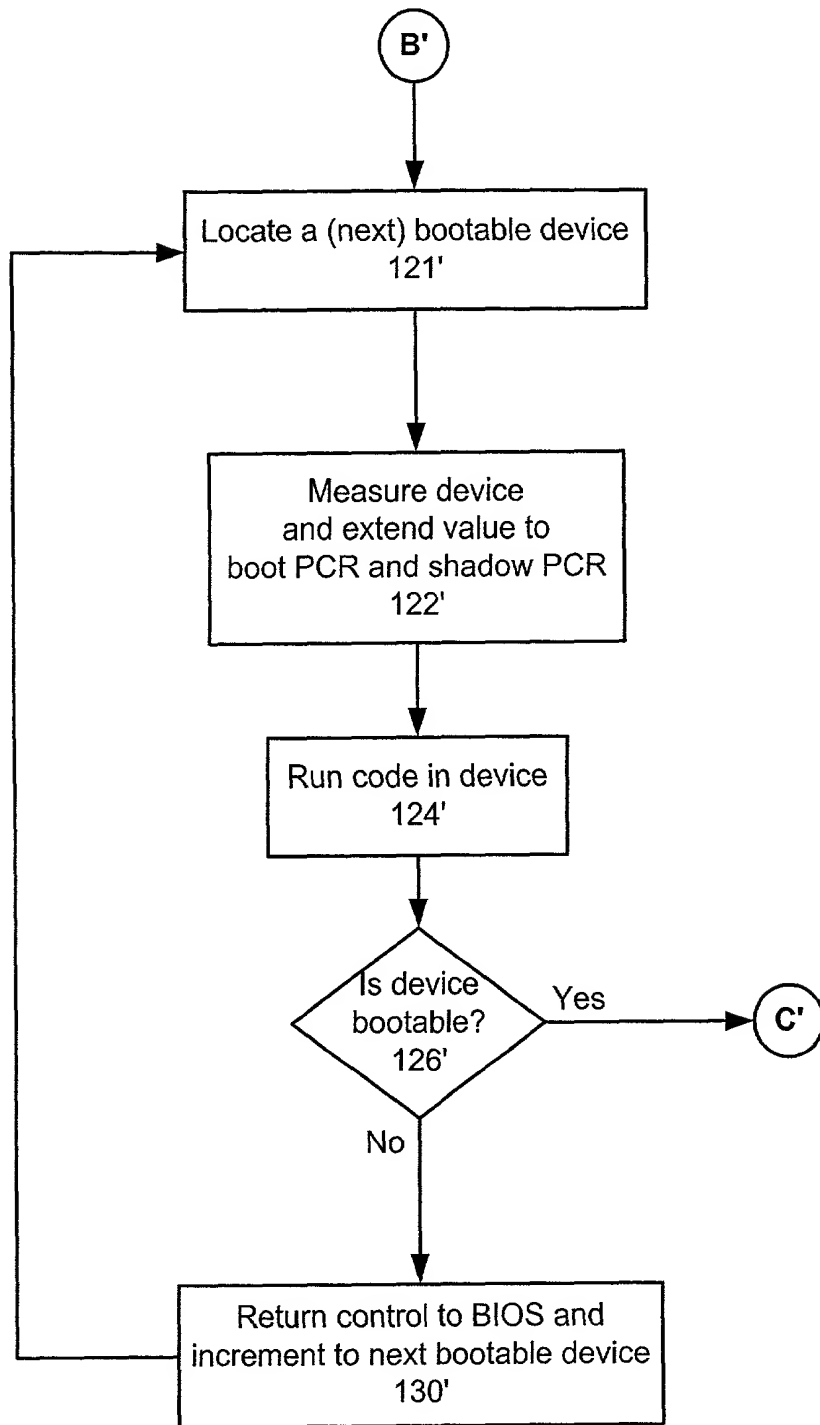


FIG. 3B

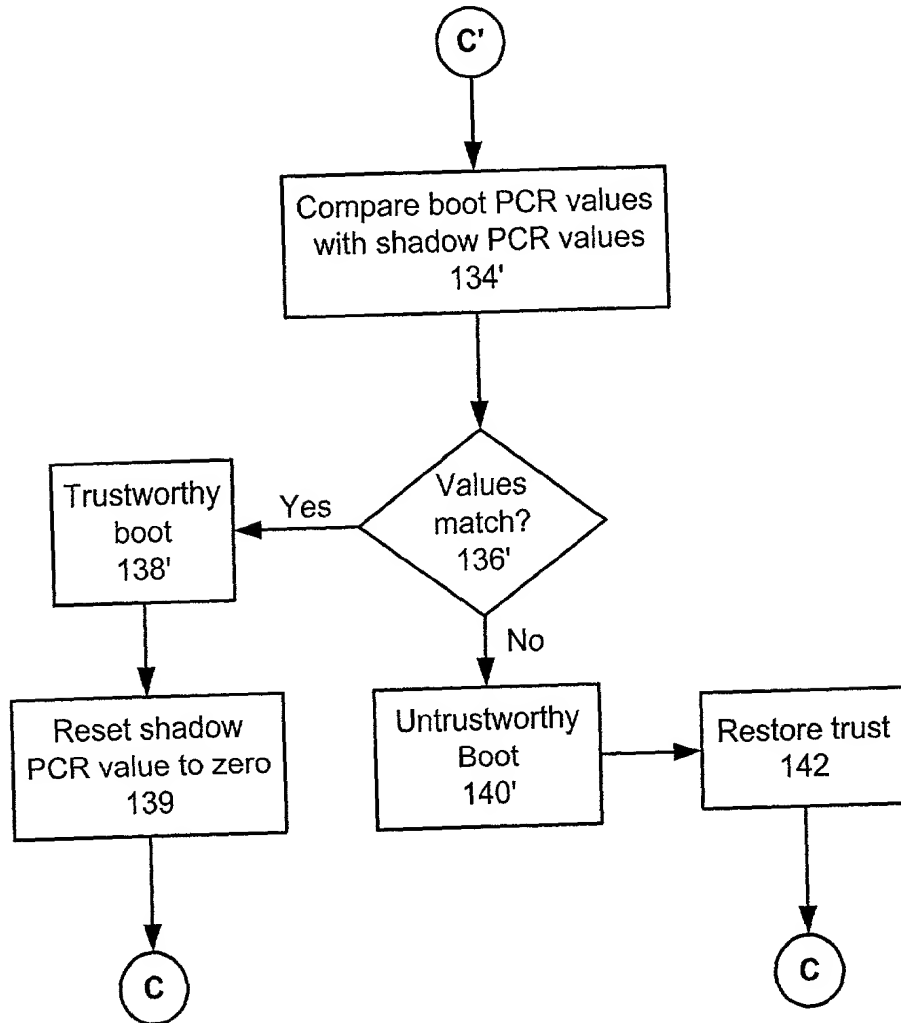


FIG. 3C